representative document it receives, certifies the resulting separate time-stamped receipt with its own verifiable cryptographic signature, and transmits the certificate back to the author. This transmittal may be directly to the requesting author or by way of the administrative TSA where the receipts are combined with or without further certification by the TSA. The combination of signature scheme and a published directory of author IDs provides verification of the utilization of the agents that were in fact selected by the pseudorandom generator. This distributed agent embodiment of the invention presents some advantages over the receiptlinking procedure in that a certified time-stamp is provided more quickly and a given author's later proof of a document is less reliant upon the availability of the certificates of other authors.

Additional variations in the process of the invention might include the accumulation of documents, preferably in hashed or other representative form, generated within an author organization over a period of time, e.g. a day or more depending upon the extent of activity, with the collection being hashed to present a single convenient document for time-stamping and certification. Also, the initial seed for the pseudorandom generator may be based upon a function of time or previously receipted documents, as well as of the document. The implementation of the process may be automated in simple computer programs which would directly carry out the described steps of hashing and transmitting original documents, selecting time-stamping agents, applying current time stamps, and returning certified receipts.

THE DRAWING

The present invention will be described with reference to the accompanying drawing of which:

FIG. **1** is a flow diagram of the general process of time-stamping a document according to the invention;

FIG. **2** is a flow diagram of a specific embodiment of the process; and

FIG. **3** is a flow diagram of another specific embodiment of the process.

DESCRIPTION OF THE INVENTION

The following examples of the application of embodiments of the present invention will serve to further describe the involved process. For convenience in the presentation of these examples, the deterministic function selected is the md4 hashing algorithm described by Rivest, as mentioned above, and the verifiable signature scheme is the public key method suggested by Diffie and Hellman, as implemented by Rivest et al. in U.S. Pat. No. 4,405,829. Further, in order to simplify explanation of the process and for the additional reasons noted below, only representative segments of the entire numbers will be employed.

The receipt-linking embodiment of the invention shown in FIG. **2** is initially considered. Although the present process may be used with documents of any length, the following apt excerpt is amply representative of a document, D_k, which an author prepares at step **21** and for which time-stamping is desired:

> Time's glory is to calm contending kings, To unmask falsehood, and bring truth to light, To stamp the seal of time in aged things, To wake the morn, and sentinel the night, To wrong the wronger till he render right;
>
> The Rape of Lucrece

By means of the md4 algorithm, the document is hashed, at optional, dashed step **22**, to a number, H_k, of a standard 128 bit format which expressed in base **16** appears as:

ef6dfdcd833f3a43d4515a9fb5ce3915

The author, A_k, whose system identification number ID_k, is 172 in a 1000 member author universe, transmits the thus-identified document to the system TSA, at step **22**, as the message, (ID_k,H_k), which appears:

172, ef6dfdcd833f3a43d4515a9fb5ce3915

as a request that the document be time-stamped.

The TSA then prepares the receipt for document, D_k, by adding, at step **25**, a sequential receipt number, r_k, of 132, for example, and a statement of the current time, t_k. This time statement might include a standard 32 bit representation of computer clock time plus a literal statement, i.e. 16:37:41 Greenwich Mean Time on Mar. 10, 1990, in order to allow the final time-stamp certificate to be easily readable by the author, A_k. The receipt would then comprise the string, (r_k,t_k,ID_k,H_k).

At this point it would be appropriate to further consider the earlier-mentioned reduction of number size to representative segments. As is described by Rivest et al. in U.S. Pat. No. 4,405,829, the cryptographic public key scheme to be employed in this example (generally known in the field as the "RSA" signature scheme) requires the division of an extended message into blocks that may each be represented by a number not exceeding the encoding key number element, n. Each such block is then signed with the RSA algorithm, to be reassembled after transmission. Therefore, in order to be able to use a number, n, of reasonable size in this example while maintaining a single block for the final receipt string to be certified with the RSA scheme, each element of the receipt string will be reduced to a representative eight bits, typically the last eight bits of any overlong string, and those bits will be stated in base **16** to present a two hexadecimal character string. Thus, for instance, the 128 bit document hash, H_k, will be represented by its last eight bits, i.e. 0001 0101, stated as 15 (base 16). Likewise, ID_k, 172, is 1010 1100 and is represented by ac (base 16). Without actually undertaking the calculation, it will suffice to assume that the time statement, t_k, is represented as **51**. The receipt number, **132**, would be represented as **84**. The receipt string to this point, i.e. (r_k,t_k,ID_k,H_k) now appears as 8451ac15.

Assume now that the immediately preceding document, D_{k-1}, was processed by the TSA as the request:

201, d2d67232a61d616f7b87dc146c575174

at 16:32:30 on Mar. 10, 1990 (t_{k-1} being represented as 64). The TSA adds these data at step **27**, to the receipt string for D_k to yield the hexadecimal representation, 8451ac1564c974. This receipt R_k, now contains data fixing the time for D_k and a time, t_{k-1}, before which author, A_k, cannot claim that D_k existed. This limitation on A_k is established by the fact that the previous author, A_{k-1}, holds a time certificate, C_{k-1}, that fixes t_{k-1} as subsequent to the linked time data, t_{k-2}, in the certificate of author, A_{k-2}, and so on for as long as a proof requires.

To establish that TSA in fact originated the receipt for document, D_k, that receipt is transmitted, at step **29**,